UNITED STATES DISTRICT COURT
WESTERN DISTRICT PENNSYLVANIA

KAREN AND MICHAEL MARTIN, individually and on behalf of all others similarly situated, Plaintiffs, v. KEYBANK NATIONAL ASSOCIATION, KEYCORP, and OVERBY-SEAWELL COMPANY, Defendants.	Case No. 2:22-cv-1346 CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiffs Karen and Michael Martin (together, "Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following against Defendants KeyBank National Association ("KeyBank"), KeyCorp (together with KeyBank, "Key"), and Overby-Seawell Company ("OSC") (collectively, "Defendants"), based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to Plaintiffs, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiffs bring this class action on behalf of consumers that suffered, and continue to suffer, injuries as a direct result of Defendants' conscious failure to take adequate and reasonable measures to protect their computer systems, which contained highly sensitive, personally identifiable information of its customers, which included customer names, mortgage property addresses, mortgage account numbers, mortgage account information, phone numbers, property information, the first eight digits of a customer's Social Security number, insurance policy numbers, and insurance information (collectively, "PII").

2. KeyBank claims on its website that "[y]our security and privacy are our highest priorities."[1] However, despite this claim, on August 4, 2022, KeyBank was contacted by one of the company's third-party vendors, OSC that an unauthorized external party had gained remote access to OSC's network and, on July 5, 2022, acquired certain information from a number of OSC clients, including PII of KeyBank clients (the "Data Breach").

3. KeyBank uses the services of OSC, a vendor that provides KeyBank ongoing verification that its residential mortgage clients are maintaining property insurance on their homes.

4. The harm resulting from a data breach such as this Data Breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk – to the extent it is even possible to do so – requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

5. Plaintiffs bring this class action for Defendants' failure to comply with industry and government regulatory standards to protect information systems that contain PII and Defendants' failure to provide adequate notice to Plaintiffs and other Class Members that their PII had been compromised in the Data Breach.

6. As a direct and proximate result of Defendants' inadequate data security, and its breach of its duty to handle PII with reasonable care, Plaintiffs and Class Members' PII has been accessed by hackers and exposed to an untold number of unauthorized individuals.

---

[1] *Information about Merchant Data Breaches*, KEYBANK https://www.key.com/about/security/merchant-data-breaches.html (last visited Sept. 19, 2022).

7. Plaintiffs and Class Members are now at a significantly increased risk of fraud, identity theft, and misappropriation of PII, the risk of which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

8. To recover from the Data Breach, Plaintiff and the Class seek from Defendants damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendants to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendants; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

A. Plaintiffs

9. Plaintiff Karen Martin ("Plaintiff K. Martin") is a resident of Allegheny County, Pennsylvania. Plaintiff K. Martin is the wife of Plaintiff Michael Martin.

10. Plaintiff Michael Martin ("Plaintiff M. Martin") is a resident of Allegheny County, Pennsylvania.

11. Plaintiffs took out a mortgage loan for a property they own in Sewickley, Pennsylvania.

12. Plaintiffs refinanced their mortgage with KeyBank in June 2019.

13. After refinancing with KeyBank, Plaintiffs' home loan is secured by a mortgage serviced by KeyBank.

14. For all times relevant to this Complaint, KeyBank was the servicer of the loan, and OSC performed services as KeyBank's vendor. Pursuant to an agreement between KeyBank and OSC, KeyBank transmitted Plaintiffs' PII to OSC.

15. Plaintiffs each received a notice letter from KeyBank, dated August 26, 2022 (the "Notice Letter"), indicating that on August 4, 2022, KeyBank was contacted by OSC, regarding the Data Breach affecting KeyBank's clients. The Notice Letter from KeyBank stated that Plaintiffs' and Class Members' PII was compromised as part of the Data Breach.

16. Plaintiffs' PII was disclosed without their authorization to unknown third parties as a result of Defendants' Data Breach.

17. Since the announcement of the Data Breach, Plaintiffs have incurred significant out-of-pocket costs, and have been required to spend their valuable time and resources in an effort to detect and prevent any additional misuses of their PII.

18. Plaintiffs would not have had to incur such costs or spend such time but for the Data Breach.

19. Plaintiffs have already spent significant time on the phone and internet, monitoring their accounts, and attempting to learn about the full extent of the Data Breach.

20. Plaintiffs would not have given their PII to Defendants if they had known that Defendants were not maintaining adequate data security protections with respect to their PII.

21. As a result of the Data Breach, Plaintiffs have and will continue to be at heightened risk for fraud and identity theft, and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

B. Defendants

22. Defendant KeyBank is a National Association organized under the laws of the United States with a principal place of business in Cleveland, Ohio. Among other things, KeyBank originates and periodically sells commercial and residential mortgage loans but continues to service those loans for the buyers of those mortgages.

23. Defendant KeyCorp is a Fortune 500 publicly-traded company incorporated in Ohio with a principal place of business in Cleveland, Ohio. KeyCorp is a bank holding company ("BHC") under the Bank Holding Company Act of 1956. KeyCorp is the parent holding company for KeyBank, its principal subsidiary, through which most of KeyCorp's banking services are provided. KeyBank operates in 15 states, including 15 locations in the Pittsburgh, Pennsylvania area.

24. KeyBank and its bank holding company KeyCorp are one of the nation's largest banks and financial services companies, with KeyCorp having consolidated total assets of approximately $186.3 billion as of December 31, 2021.

25. As of December 31, 2021, KeyBank had approximately 999 full-service retail banking branches and a network of 1,317 ATMs in 15 states.

26. KeyBank provides traditional banking and lending services to its customers including originating and/or servicing residential mortgages.

27. According to KeyCorp's U.S. Securities and Exchange Commission ("SEC") Form 10-K for fiscal year ending December 31, 2021, filed on February 22, 2022 ("2021 10-K"):

> Through KeyBank and certain other subsidiaries, we provide a wide range of retail and commercial banking, commercial leasing, investment management, consumer finance, student loan refinancing, commercial mortgage servicing and special servicing, and investment banking products and services to individual, corporate, and institutional clients through two major business segments: Consumer Bank and Commercial Bank.

28. According to KeyCorp's 2021 10-K, its "residential mortgage portfolio is comprised of loans originated by our Consumer Bank primarily within our 15-state footprint and is the largest segment of our consumer loan portfolio as of December 31, 2021, representing approximately 51% of consumer loans."

29. Defendant OSC is a Georgia corporation with a principal place of business in Kennesaw, Georgia.

30. OSC is a technology services vendor of KeyBank that provides KeyBank ongoing verification regarding its residential mortgage clients' maintenance of property insurance, which are required for homeowners to maintain based on the terms of the mortgage.

31. According to OSC's website, "[a]t the core of all we do is a strict adherence to compliance best practices, [and] rigorous security on and off-line."[2]

JURISDICTION AND VENUE

32. The Court has subject-matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. §1332(d), because Plaintiffs and Defendants are citizens of different states and the amount in controversy exceeds $5,000,000.

33. The Court also has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. §1367(a) because the state law claims are related to claims in the action within such original jurisdiction and they form part of the same case or controversy under Article III of the U.S. Constitution.

34. This Court has personal jurisdiction over KeyBank because (1) KeyBank actively markets its banking products, including mortgages, and conducts a substantial business in and throughout Pennsylvania, where there are a considerable number of KeyBank branches and customers; including in the following towns/cities: Ambler, Bethel Park, Bridgeville, Butler, California, Conshohocken, Coraopolis, Corry, Cranberry Township, Devon, Downingtown, Doylestown, Dresher, East Norriton, Elizabeth, Emmaus, Erie, Exton, Frazer, Gibsonia, Gilbertsville, Greensburg, Harleysville, Houston. Huntingdon Valley, Imperial, Ingomar, Kennett Square, Lansdale, Lansford, Lehighton, Limerick, Maple Glen, McKees Rocks, McMurray,

[2] *What We Do*, OSC INSURANCE SERVICES, https://www.oscis.com/who-we-are/what-we-do/ (last visited Sept. 19, 2022).

Monongahela, Monroeville, Mount Pleasant, Natrona Heights, New Kensington, Norristown, North East, North Huntingdon, North Wales, Oakmont, Palmerton, Philadelphia, Pittsburgh, Plymouth Meeting, Pottstown, Quakertown, Red Hill, Sellersville, Sewickley, Skippack, Slatington, Souderton, Spring House, Trexlertown, Uniontown, Walnutport, Warminster, Warren, Warrington, Washington, West Chester, Wexford, Whitehall, and Willow Grove. Thus, the wrongful acts alleged in the Complaint caused harm to Plaintiffs and Class Members in part, in Pennsylvania.

35. This Court has personal jurisdiction over KeyCorp because (1) KeyCorp actively markets its financial services and products and conducts a substantial business in and throughout Pennsylvania, where there are a considerable number of KeyBank branches and customers; and (2) the wrongful acts alleged in the Complaint caused harm to Plaintiffs and Class Members in Pennsylvania.

36. This Court has personal jurisdiction over OSC because (1) OSC actively markets its services to clients in Pennsylvania and conducts a substantial business in and throughout Pennsylvania, where it provides KeyBank technology and verification services for its residential mortgages; and (2) the wrongful acts alleged in the Complaint caused harm to Plaintiffs and Class Members in Pennsylvania.

37. Venue is proper in this District, pursuant to 28 U.S.C. §1391(b)(2), because a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

38. On July 26, 2022, KeyBank issued the Notice Letter which stated that OSC informed KeyBank that an "unauthorized external party" had gained remote access to OSC's

network, and on July 5, 2022, acquired certain information from a number of OSC clients, including certain personal information of KeyBank clients. This PII included names, mortgage property addresses, mortgage account numbers and mortgage account information, phone numbers, property information, the first eight digits of Social Security numbers, and home insurance policy number and home insurance information belonging to Plaintiffs and Class Members.

39. The "certain information" that was acquired included names, mortgage property addresses, mortgage account number(s) and mortgage account information, phone numbers, property information, the first eight digits of Social Security numbers, and home insurance policy numbers and home insurance information (collectively, "PII").

40. PII pertaining to Plaintiffs' KeyBank mortgage was part of the data acquired by unauthorized third parties from OSC's systems in the Data Breach.

41. The Notice Letter states that "OSC is investigating this incident with the assistance of third-party cybersecurity experts" as well as the Federal Bureau of Investigation ("FBI"). Because the investigation is not yet completed, additional items of PII as well as other facts surrounding the Data Breach may be uncovered or have already been uncovered and not yet publicly disclosed.

42. The Notice Letter states that since discovering the Data Breach, OSC has "deployed enhanced security monitoring tools across their network." These are steps that should have been employed in the first place and which would have prevented or limited the impact of the Data Breach.

43. Discovery of Defendants, law enforcement, investigators, and OSC's "third-party cybersecurity experts" will reveal more specific facts about Defendants' deficient and unreasonable security procedures.

44. The Notice Letter states that affected customers should obtain credit monitoring and identity theft protection services to help them detect possible misuse of PII, which KeyBank is providing for only two years.

45. As a result of the Data Breach, Plaintiffs and Class Members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

B. Data Security Industry Standards

46. Defendants are well aware of the importance of safeguarding Plaintiffs' and Class Members' PII, and that by virtue of their business, they place Plaintiffs' and Class Members' PII at risk of being targeted by cybercriminals.

47. Defendants are aware that the PII that they collect, organize, and store, can be used by cybercriminals to engage in crimes such as identity fraud and theft using Plaintiffs' and Class Members' PII.

48. For example, OSC's website states, "[f]or many clients, our daily routine involves the secure handling of hundreds of thousands of complex and interrelated data points. We do this work with sophisticated technology, proven processes and smart people."[3]

[3] *Our Way*, OSC INSURANCE SERVICES, https://www.oscis.com/who-we-are/our-way/ (last visited Sept. 19, 2022).

49. For example, according to KeyCorp's 2021 10-K, the company recognizes such cybersecurity risks on the part of its technology service vendors like OSC when it says:

> We also face risks related to the increasing interdependence and interconnectivity of financial entities and technology systems. ***A technology failure, cyberattack or other security breach that significantly compromises the systems of one or more financial parties or service providers could have a material impact on counterparties or market participants, including us. Any third-party technology failure, cyberattack, or security breach could adversely affect our ability to effect transactions, service clients, or otherwise operate our business***.
>
> * * *
>
> We rely on third parties to perform significant operational services for us.
>
> ***Third parties perform significant operational services on our behalf***. Additionally, some of our third parties outsource aspects of their operations to other third parties (commonly referred to as "fourth parties"). These parties are subject to similar risks as Key relating to cybersecurity and breakdowns or failures of their own systems, internal processes and controls, or employees. ***One or more of these third parties may experience a cybersecurity event or operational disruption and, if any such event does occur, it may not be adequately addressed, either operationally or financially, by such third party***. Certain of these third parties may have limited indemnification obligations or may not have the financial capacity to satisfy their indemnification obligations. Financial or operational difficulties of a third party could also impair our operations if those difficulties interfere with such third party's ability to serve us. Additionally, some of our outsourcing arrangements are located overseas and, therefore, are subject to risks unique to the regions in which they operate. If a critical third party is unable to meet our needs in a timely manner or if the services or products provided by such third party are terminated or otherwise delayed and if we are not able to identify or develop alternative sources for these services and products quickly and cost-effectively, it could have a material adverse effect on our business. Additionally, regulatory guidance adopted by federal banking regulators related to how banks select, engage, and manage their third parties affects the circumstances and conditions under which we work with third parties and the cost of managing such relationships.

[Emphasis added.]

50. According to KeyCorp's SEC Form 10-Q for fiscal quarter ending June 30, 2022, filed on August 2, 2022, filed just days before OSC informed Key, KeyCorp states:

> ***Cyberattack risks may also occur with our third-party technology service providers*** and may result in financial loss or liability that could adversely affect our

> financial condition or results of operations. Cyberattacks could also interfere with third-party providers' ability to fulfill their contractual obligations to us. ***Recent high-profile cyberattacks have targeted retailers, credit bureaus, and other businesses for the purpose of acquiring the confidential information (including personal, financial, and credit card information) of their customers***. Recently, there have also been numerous highly publicized cases where hackers requested ransom payments in exchange for not disclosing customer information or to restore company access to locked systems. We may incur expenses related to the investigation of such attacks or related to the protection of our customers from identity theft as a result of such attacks. We may also incur expenses to enhance our systems or processes to protect against cyber or other security incidents. ***Risks and exposures related to cyberattacks are expected to remain high for the foreseeable future due to the rapidly evolving nature and sophistication of these threats, as well as due to the expanding use of Internet banking, mobile banking, and other technology-based products and services by us and our clients***. To date, Key has not experienced material disruption of our operations, or material harm to our customers, as a result of the heightened threat landscape of cyberattacks.

[Emphasis added.]

51. Because Defendants failed to implement, maintain, and comply with necessary cybersecurity requirements, Defendants were unable to protect Plaintiffs' and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

52. As a proximate result of such failures, cybercriminals gained unimpeded and unauthorized access to Defendants' network and acquired Plaintiffs' and Class Members' PII in the Data Breach.

53. Only after discovering the Data Breach did Defendants begin to undertake basic steps recognized in the industry to protect Plaintiffs' and Class Members' PII.

54. Defendants were unable to prevent the Data Breach and were unable to detect the unauthorized access to vast quantities of sensitive and protected files containing Plaintiffs' and Class Members' PII.

55. Commonly accepted data security standards among businesses that store personal and financial information, such as the PII involved here, include, but are not limited to:

(a) Maintaining a secure firewall configuration;

(b) Monitoring for suspicious or irregular traffic to servers;

(c) Monitoring for suspicious credentials used to access servers;

(d) Monitoring for suspicious or irregular activity by known users;

(e) Monitoring for suspicious or unknown users;

(f) Monitoring for suspicious or irregular server requests;

(g) Monitoring for server requests for personal and financial information;

(h) Monitoring for server requests from VPNs; and

(i) Monitoring for server requests from Tor exit nodes.

56. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity (*Start with Security: A Guide for Business* (June 2015)) and protection of personal and financial information (*Protecting Personal Information: A Guide for Business* (Oct. 2016)), which includes basic security standards applicable to all types of businesses.

57. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by §5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

58. Since Defendants were entrusted with Plaintiffs' and Class Members' PII, they had and continue to have a duty to keep the PII secure.

59. Plaintiffs and Class Members reasonably expect that when they provide their PII to KeyBank, KeyCorp, and its vendors (OSC), Plaintiffs' and Class Members' information will be safeguarded.

60. Despite Defendants' obligations, Defendants failed to appropriately monitor and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

61. Key also negligently entrusted duties to safeguard Plaintiffs' and Class Members' PII to OSC without adequately monitoring, inspecting, and controlling OSC's data security practices.

62. Key also negligently supervised OSC and failed to require OSC to implement, maintain, and upgrade sufficiently its data security systems and protocols.

63. Had Defendants properly maintained their systems and adequately protected them, they could have prevented the Data Breach.

C. Defendants Violated Their Common Law Duty of Reasonable Care

64. Defendants are aware of the importance of security in maintaining personal information (particularly sensitive personal and financial information like the PII involved here), and the value consumers place on keeping their PII secure.

65. In addition to obligations imposed by federal and state law, Defendants owed and continue to owe a common law duty to Plaintiffs and Class Members – who entrusted Defendants with their PII – to exercise reasonable care in receiving, maintaining, and storing, the PII in Defendants' possession.

66. Defendants owed and continue to owe a duty to prevent Plaintiffs' and Class Members' PII from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendants' duty was (and is) the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure information

technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiffs' and Class Members' PII.

67. Defendants owed a duty to Plaintiffs and Class Members, who entrusted Defendants with extremely sensitive PII, to design, maintain, and test the information technology systems that housed Plaintiffs' and Class Members' PII, to ensure that the PII in Defendants' possession was adequately secured and protected.

68. Defendants owed a duty to Plaintiffs and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the PII stored in Defendants' systems. In addition, this duty also required OSC to adequately train its employees and others with access to Plaintiffs' and Class Members' PII on the procedures and practices necessary to safeguard such sensitive information. This duty also required supervision, training, and compliance on Key's part to ensure that its vendor, OSC, complied with creating, implementing, and maintaining reasonable data security practices and procedures sufficient to protect Plaintiffs' and Class Members' PII.

69. Defendants owed a duty to Plaintiffs and Class Members to implement processes that would enable Defendants to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

70. Defendants owed a duty to Plaintiffs and Class Members to disclose when and if OSC's information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiffs' and Class Members' PII.

71. Defendants violated these duties. For example, the Notice Letter fails to notify Plaintiffs and Class Members ***when*** OSC exactly became aware of the Data Breach. The Notice

Letter only states that on July 5, 2022, an "unauthorized external party" acquired the PII of OSC's clients. The Notice Letter further states that Key became aware of it on August 4, 2022, after OSC informed them. Plaintiffs, Class Members, and the public did not learn of the breach until August 26, 2022, when the Notice Letters were mailed out. Defendants failed to publicly describe the full extent of the Data Breach and notify affected parties. This demonstrates that Key did not properly supervise OSC and OSC did not implement measures designed to timely detect a breach of its information technology systems, as required to adequately safeguard Plaintiffs' and Class Members' PII.

72. Defendants also violated their duty to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiffs' and Class Members' PII.

73. As the Notice Letter states, "OSC is investigating this incident with the assistance of third-party cybersecurity experts. They have deployed enhanced security monitoring tools across their network and notified the Federal Bureau of Investigation (FBI) of this incident." The Notice Letter says nothing ***of what Key is doing*** to investigate its customers' PII falling into the hands of cybercriminals. OSC could have taken these steps ***beforehand*** to protect the PII in its possession and prevent the Data Breach from occurring, as required under FTC guidelines, as well as other state and federal law and/or regulations.

74. Defendants owed a duty to Plaintiffs and Class Members to timely disclose the fact that a data breach, resulting in unauthorized access to their PII, had occurred.

D. The Value of Private Information and Effects of Unauthorized Disclosure

75. Defendants were well aware that the protected PII they acquire, store, and utilize is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

76. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former U.S. Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[4] The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld.

77. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "'[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud.'"[5]

78. The forms of PII involved in this Data Breach are particularly concerning, including: ***Social security numbers*** – unlike credit or debit card numbers in a payment card data breach – which can quickly be frozen and reissued in the aftermath of a breach – unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

---

[4] William P. Barr, Attorney General, DEP'T OF JUST., *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax* (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

[5] Priscilla Liguori, *Legislator, security expert weigh in on Rutter's data breach*, ABC27 (Feb. 14, 2020), https://www.abc27.com/local-news/york/legislator-security-expert-weigh-in-on-rutters-data-breach/.

79. Indeed, even the Social Security Administration warns that the process of replacing a social security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you shouldn't use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.[6]

80. Social security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit – among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

81. Furthermore, a social security number consists of nine (9) numbers (*i.e.*, XXX-XX-XXXX). Here the exfiltrated PII included the ***first eight (8) digits of a customer's social security number***. Cybercriminals could easily guess Plaintiffs' and Class Members' remaining number by

[6] Publication No. 05-10064, *Identify Theft and Your Social Security Number*, Social Security Administration (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

cycling through 1 through 0 until it hits. Thus, there is essentially no difference on the part of cybercriminals between stealing the first eight digits or the full social security number.

82. ***Financial account information*** – Stolen financial account can have an equally devasting impact on consumers. Cybercriminals can deplete and wipe out a person's life savings or take out a loan or mortgage against someone's home with the click of a button. Here the exfiltrated PII included financial account information such as Plaintiffs' and Class Members' ***mortgage account number(s) and mortgage account information*** **coupled with** ***property information***.

83. The ramifications of exfiltrating this form of PII is equally as devasting as it can lead to mortgage and title fraud as described below. Real estate fraud is one of the fastest growing cybercrimes in America. According to FBI Special Agent Siobhan Johnson, "'[r]eal estate fraud is one of the fastest growing cyber scams across the country.'"[7] Between 2018 to 2020, the FBI saw approximately a 42% increase in the percentage of real estate crimes.

84. A home's title and mortgage information are often stored and available online. Criminals use this information to transfer a person off his or her home's title. This is only made easier with the PII that was stolen – ***mortgage account number(s) and mortgage account information***. Often it is just a quick trip to the county recorder's office to file the "updated" forged paperwork. Also, with the convenience of being online, many county offices allow paperwork to be submitted electronically. Once filed, the majority of county recorder's offices assume that the paperwork is genuine, and the actual property owner is informed. Unfortunately, there is no

[7] *References*, NATIONAL ASSOCIATION OF REALTORS, https://www.nar.realtor/references-147 (last visited Sept. 19, 2022).

uniform or consistent system to authenticate the filed paperwork. Criminals can then take out massive loans using a home's equity, leaving the homeowner on the hook.

85. Further, criminals can use the information to devise and employ phishing and social engineering schemes capitalizing on the genuine information stolen from Defendants to send fraudulent mail, emails, and other communications to Plaintiffs and Class Members that look authentic, but which are designed to lure them into paying money or providing other information that the criminals can use to steal money. For example, homeowners with trouble paying their loan payments may experience scams targeting them.

86. According to *Experian*:

> Mortgage Foreclosure Relief and Debt Management Scams
>
> In this type of mortgage fraud, scammers contact homeowners offering help if they can't make payments or may be falling behind on their mortgage (the primary contact is by phone with these). . . .
>
> Often they make promises of lower payments or making the payments for a homeowner in exchange for rent payments to their company. However, they don't actually make the mortgage payments and you may end up going into foreclosure anyway. Also known as foreclosure scams or foreclosure rescue schemes, this kind of fraud is unfortunately very common and can cost consumers a lot of money.[8]

87. The information stolen in the Data Breach, by itself, can also be used by criminals to perpetrate fraud. *Experian* explains that certain scams, including mortgage fraud, can be effectively perpetrated using only the PII involved here – ***a name, social security number, and mortgage account number***:

> How Consumers Are Affected By Mortgage Fraud
>
> Identity theft is a particularly threatening form of mortgage fraud, as it tends to lead directly toward homeowner financial loss. ***For example, if an identity thief***

[8] Brian O'Connell, *Here's Everything You Need to Know About the Risks of Mortgage Fraud*, EXPERIAN (Apr. 18, 2018), https://www.experian.com/blogs/ask-experian/heres-everything-you-need-to-know-about-the-risks-of-mortgage-fraud/#:~:text=Mortgage%20Foreclosure%20Relief%20and%20Debt,is%20by%20phone%20with%20these).

> ***steals a homeowner's Social Security number, or intercepts the mortgage account number***, he or she can use that information to take out a home equity line of credit (also known as a HELOC) worth tens of thousands of dollars, in the homeowner's name.[9]

[Emphasis added.]

88. *Experian* explains how mortgage fraud impacts the homeowner. When the credit is provided to the fraudster:

> The cash is sent to a fraudulent account established by the thief, and the homeowner is left holding the bill. Or, the fraudster could take out a second mortgage using the homeowner's stolen data information, and escape with the cash, once again leaving the debt to the homeowner.
>
> While any form of mortgage fraud is a serious offense, losing one's data to identity thieves can trigger a financial loss that's difficult to overcome, and that could take years to clear. Additional impacts include losing money, time, or missing out on the purchase of a dream home because you have to take additional time to deal with restoring your identity if you're the victim of mortgage fraud.[10]

89. *Identity Force* explains what a thief or scammer can do with sensitive information, such as loan information and identifying details, including stealing your home:

> Mortgaging Your Good Name
>
> Mortgage fraud through identity theft is a very real risk. A thief can steal your Social Security number and other identifying details, then pretend to be you to a bank or mortgage broker. The criminal might refinance your home for more than what's owed and then take the extra cash or obtain a home equity line of credit and drain that account.
>
> Thieves can get the information they need for these transactions by stealing your mail, getting personal details through fraudulent phone calls or making copies of your . . . driver's license to impersonate you. Unfortunately, sometimes it's friends and family who are the culprits (known as familiar fraud) since they may have access to files inside a home and often know many of the personal details required to impersonate you.[11]

---

9 *Id*.

10 *Id.*

11 *Is Your Home at Risk to Identity Thieves?* IDENTITYFORCE: A TRANSUNION BRAND (Jan. 12, 2022), https://www.identityforce.com/blog/home-loan-identity-theft.

90. The five year "Home Lock" protection service that Plaintiffs purchased immediately after and as a result of the Data Breach was especially meant to combat this type of fraud.

91. ***Insurance information*** – stolen insurance information, such as the PII that was involved here – ***home insurance policy number*** **and** ***home insurance information*** – can also result in cybercriminals taking out fraudulent insurance policies or submitting fraudulent insurance in a person's name.

92. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII secure are long-lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

93. Thus, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if their systems were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

94. Compared to other data breaches, the types of PII involved in this Data Breach are incredibly comprehensive and sensitive, as they contain virtually every form of PII available for a person (*i.e.*, names, social security numbers, addresses, mortgage account number(s), and mortgage account information).

95. Whereas in other data breaches where exfiltrated PII is semi-compartmentalized and only involves a few forms of PII (such as just names and credit card numbers or names and

bank account numbers), here, such a comprehensive dataset is even more valuable to cybercriminals who can use Plaintiffs' and Class Members' PII to commit a host of identity theft and fraud.

96. As highly sophisticated parties that handle sensitive PII, Defendants failed to establish and/or implement appropriate administrative, technical, and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII to protect against anticipated threats of intrusion of such information.

97. Identity thieves use stolen PII for various types of criminal activities, such as when personal and financial information is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud, and government fraud.

98. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are other ways for cybercriminals to exploit information they already have in order to get even more PII from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

99. There is often a lag time between when fraud occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that

> information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[12]

100. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

101. Plaintiffs and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

102. Thus, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

103. Data breaches are preventable. As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised." "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

104. Here Defendants claim to have "deployed enhanced security monitoring tools across their network" after the Data Breach, but should have implemented them in advance to prevent the Data Breach.

---

[12] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches and Identity Theft* (June 2007).

105. The types of information compromised in the Data Breach are immutable. Plaintiffs and Class Members are not able to change them or simply cancel them, like a credit card, to avoid harm or fraudulent use of the information. Just like a birthdate or a mother's maiden name, these pieces of information cannot be changed by logging into a website and changing them in settings, and they can be used alone or in conjunction with other pieces of Plaintiffs' and Class Members' information to commit serious identity theft and fraud.

E. Defendants Obtain, Collect, and Store Plaintiffs' and Class Members' PII

106. In the ordinary course of doing business as a financial institution, Key requires its customers to provide their sensitive PII in order to obtain a mortgage. The mortgage requires a homeowner to obtain homeowners/property insurance. That is where OSC comes in. Key utilizes OSC to conduct its verification process of its clients to ensure they properly maintain property insurance. Thus, Key provided Plaintiffs' and Class Members' PII to OSC.

107. The Notice Letter indicates that broad categories of information, such as "mortgage account information'' and "home insurance information" were acquired by cybercriminals but does not provide any more particularity regarding what information those categories encompass. In addition, the Notice Letter explains that OSC continues to investigate the Data Breach as of August 26, 2022. The logical inference is that additional information regarding the Data Breach is yet to be uncovered, which may reveal additional misconduct or other fields of valuable information not already specified.

108. By obtaining, using, disclosing, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

109. Thus, Defendants had access to Plaintiffs' and Class Members' PII which was stored on their systems.

110. Plaintiffs and Class Members reasonably expected that their mortgage servicer (and its vendors) would use the utmost care to keep their PII confidential and securely maintained.

111. Key acknowledges in its Notice Letter to Plaintiffs and Class Members its obligation to protect and secure PII: "Your business is important to us, and the security of your accounts and personal information is something we take very seriously. . . . Keeping your personal information safe and secure is of utmost importance to us."

112. Despite Defendants' obligation to protecting personal information, Defendants failed to prioritize data and cybersecurity by adopting reasonable data and cybersecurity measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' PII.

113. Had Defendants remedied the security deficiencies, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendants would have prevented intrusion into its information systems and, ultimately, the theft of Plaintiffs' and Class Members' PII.

F. Key Is Subject to and Failed to Comply with the GLBA

114. The Gramm-Leach-Bliley Act ("GLBA"), states that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. §6801(a).

115. A "financial institution" is defined as "any institution the business of which is engaging in financial activities as described in section 1843(k) of Title 12." 15 U.S.C. §6809(3)(A). KeyBank and KeyCorp are considered financial institutions for purposes of the GLBA. *See* 12 U.S.C. §1843(k)(4).

116. "[N]onpublic personal information" means "personally identifiable financial information . . . provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution." 15 U.S.C. §6809(4)(A). The PII involved in the Data Breach, constitutes "nonpublic personal information" for purposes of the GLBA.

117. Key collects "nonpublic personal information," as defined by 15 U.S.C. §6809(4)(A), 16 C.F.R. §313.3(n), and 12 C.F.R. §1016.3(p)(1). Accordingly, during the relevant time period, Key was subject to the requirements of the GLBA, 15 U.S.C. §§6801, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

118. The Safeguards Rule, which implements §501(b) of the GLBA, 15 U.S.C. §6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§314.3, 314.4. As alleged herein, Key violated the Safeguards Rule.

119. Key failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

120. Key's conduct resulted in a variety of failures to follow GLBA mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the Data Breach demonstrates that Key failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the PII it maintained in its data systems, instead outsourcing such responsibilities to OSC.

121. Had Key implemented data security protocols, the consequences of the data exposure could have been avoided, or at least significantly reduced as the exposure could have been detected earlier, the amount of PII compromised could have been greatly reduced, and affected consumers could have been notified – and taken protective/mitigating actions – much sooner.

G. Defendants Failed to Comply with FTC Act

122. Defendants are prohibited by the FTC Act, 15 U.S.C. §45 from engaging in "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. §45(a)(1). The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

123. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates the FTC Act.

124. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

125. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

126. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

127. Defendants are aware of and failed to follow the FTC guidelines and failed to adequately secure PII. For example, the Notice Letter explicitly references the FTC and the resources it provides regarding the prevention of identity theft. Furthermore, by failing to have reasonable data security measures in place, Defendants engaged in an unfair act or practice within the meaning of §5 of the FTC Act.

128. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

unfair act or practice prohibited by §5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

129. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals constitutes an unfair act or practice prohibited by §5 of the FTC Act.

130. Defendants were at all times fully aware of their obligations to protect the PII of consumers because of their business of obtaining, collecting, and storing PII. Defendants were also aware of the significant repercussions that would result from their failure to do so.

H. Defendants Violated Their Own Privacy Policies

131. Plaintiffs and Class Members entrusted Defendants with an extensive amount of their sensitive PII. Defendants understand the importance of protecting such information and tout their cybersecurity capabilities as a selling point.

132. For example, in its website Privacy Policy, OSC states:

> The privacy of personal client information is important to Breckenridge IS, LLC, and its subsidiaries and affiliates (collectively "Breckenridge IS" including the Overby-Seawell Co. called "OSC"). Under Federal law, any financial institution, directly or through its affiliates, is generally prohibited from sharing nonpublic personal information about consumers or customers with a nonaffiliated third party unless the institution provides such consumer or customer with a notice of its privacy policies and practices, such as the type of information that it collects from consumers and customers and the categories of persons or entities to whom the information may be disclosed. In compliance with Federal law and the state laws relating to privacy in the insurance industry, and in order to notify our clients of our privacy policies and practices, we have established this Privacy Policy.
>
> * * *
>
> Disclosing Information
>
> We do not disclose any nonpublic personal information, including financial information, about our Participants or former Participants to any third parties, except as stated in this policy, as otherwise required by law or as otherwise may be

> authorized by you from time to time. We may share this information outside Breckenridge IS or its affiliate OSC in order to process or complete, or otherwise in connection with, the transaction for which the information was provided or as otherwise authorized by our Participants. The law permits us to share this information with our affiliates. We also may disclose any of the information we collect to companies that perform marketing services on our behalf or to companies with which we have joint marketing agreements.
>
> Confidentiality and Security of Information
>
> We restrict access to nonpublic personal information about Participants to those employees of Breckenridge IS and OSC who need to know that information in order to provide products or services to our Participants. ***We have in place physical, electronic, and procedural safeguards in order to protect any nonpublic personal information we maintain regarding our Participants***.
>
> Professional Standards
>
> Whatever the legal environment, we have constantly held ourselves to the highest of professional standards. At Breckenridge IS and OSC, we strive always to maintain the highest level of confidentiality for our Participants.[13]

[Emphasis added.]

133. Despite these promises to protect its customers' PII, OSC failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to Plaintiffs' and Class Members' PII.

134. Similarly, Key represents on its Privacy and Security page that "[w]e take the security of your data and information seriously. That's why we use sophisticated tools, technology and training to keep the information you entrust to us safe, protected and secure."[14]

135. Key goes onto say:

> To safeguard your information, we also use:

---

[13] *Privacy Policy*, OSC INSURANCE SERVICES, https://www.oscis.com/privacy/ (last visited Sept. 19, 2022).

[14] *Privacy & Security*, KEYCORP, https://www.key.com/about/security/privacy-security.html (last visited Sept. 19, 2022).

- Industry-leading cybersecurity tools, practices and technology
- Multifactor identification practices that protect clients' identities
- Our Cyber Defense Center, which tracks the latest threats
- Our Fraud Prevention Services group, which monitors client accounts proactively for suspicious activity.[15]

136. Key's Online Privacy Statement states "personal information" "may be shared with third parties for Key's business purposes and to comply with applicable law." Here the PII was shared with an "unauthorized external party."[16]

137. Key's Online Privacy Statement goes on to say "we are committed to safeguarding personal information. We use physical, technical, and administrative security measures that comply with applicable federal and state laws and regulations. . . . Additional details on how Key protects information online . . . can be found on the Privacy & Security page on key.com."[17]

138. Despite these promises to protect its customers' PII, Key failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to Plaintiffs' and Class Members' PII.

139. Defendants' failure to implement appropriate security measures and adequately safeguard Plaintiffs' and Class Members' PII violated the terms of their own policies.

I. Plaintiffs and Class Members Suffered Damages

140. The ramifications of Defendants' failure to keep PII secure are long-lasting and severe. Victims of data breaches are more likely to become victims of identity fraud, occurring 65

---

15 *Id*.

16 *KeyCorp Online Privacy Statement*, KEYCORP (Feb. 4, 2020), https://www.key.com/about/misc/online-privacy-statement.html.

17 *See id*.

percent of the time. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.

141. Plaintiffs and Class Members have faced a substantial and imminent risk of identity theft and fraud as a result of the Data Breach. Unauthorized third parties carried out the Data Breach and stole the personal information of Plaintiffs and Class Members with the intent to use it for fraudulent purposes and/or sell it to other cybercriminals.

142. The risk of identity theft is particularly substantial when sensitive PII such as Social Security numbers are compromised along with other personally-identifying information.

143. Plaintiffs and Class Members have already spent and will spend substantial amounts of their money and time monitoring their accounts for identity theft and fraud and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming.

144. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

145. Further, Plaintiffs and Class Members have incurred and will incur out-of-pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

146. Besides the monetary damage sustained in the event of identity theft, consumers may also spend anywhere from approximately seven hours to upwards of over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that

"among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[18]

147. Despite all of the publicly-available knowledge of the continued compromises of PII and the importance of securing such information, Defendants' commitment to secure their customers' information fell by the wayside.

148. Key was well aware of the requirements and obligations to secure PII. Similarly, OSC as Key's vendor, was also aware of the requirements and obligations to secure PII that had been entrusted to it by Key. Further, OSC had control over the configuration and design of its own systems, and knowingly chose to forego the necessary data protection techniques needed for it to secure Plaintiffs' and Class Members' PII.

149. As a result of Defendants' failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer injuries, including out-of-pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their PII being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their PII; and continued risk to Plaintiffs' and the Class Members' PII, which remains in the possession of Defendants, and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII that was entrusted to them.

---

[18] Erika Harrell & Lynn Langton, *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUST.: OFF. OF JUST. PROGRAMS (Dec. 2013), https://www.ojp.gov/library/publications/victims-identity-theft-2012.

CLASS ALLEGATIONS

150. Plaintiffs bring this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following nationwide class:

> All individuals in the United States and its territories whose PII was disclosed by Defendants to unauthorized third parties in the data breach event publicly disclosed in August 2022.

151. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

152. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

153. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual Members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court.

154. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendants' records, including but not limited to, the information implicated in the Data Breach.

155. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

(a) Whether and to what extent Defendants had a duty to secure and protect the PII of Plaintiffs and Class Members;

(b) Whether Defendants were negligent in collecting and disclosing Plaintiffs' and Class Members' PII;

(c) Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

(d) Whether Defendants took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

(e) Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

(f) Whether Defendants breached their duties to exercise reasonable care in handling Plaintiffs' and Class Members' PII in the manner alleged herein, including failing to comply with industry standards;

(g) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

(h) Whether Defendants had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

(i) Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

(j) Whether Plaintiffs and Class Members are entitled to declaratory judgment under 28 U.S.C. §§2201, *et seq.*;

(k) Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

(l) Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

156. The requirements of Rule 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of Class Members. The claims of the Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendants to safeguard PII. Plaintiffs and Class Members each had his or her PII disclosed by Defendants to an unauthorized third party.

157. The requirements of Rule 23(a)(4) are satisfied. Plaintiffs are an adequate representative of the Class because their interests do not conflict with the interests of the Class Members. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each Member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiffs and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each Member of the Class. Defendants' uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class Member.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(Against All Defendants)

158. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

159. Defendants owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

160. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' systems to ensure that Plaintiffs' and Class Members' PII in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by their own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry and governmental regulator standards.

161. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

162. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

163. Defendants had a duty not to engage in conduct that creates a foreseeable risk of harm to Plaintiffs and Class Members.

164. Defendants breached the duties owed to Plaintiffs and Class Members and thus were negligent. Specifically, Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry and governmental regulator standards; and (d) disclose that Plaintiffs' and Class Members' PII in Defendants' possession had been or was reasonably believed to have been, stolen or compromised.

165. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' PII would not have been compromised.

166. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered injuries, including:

(a) Theft of their PII;

(b) Costs associated with requested credit freezes;

(c) Costs associated with the detection and prevention of identity theft;

(d) Costs associated with purchasing credit monitoring and identity theft protection services;

(e) Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of Defendants' Data Breach;

(f) The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being disclosed to cybercriminals;

(g) Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the societal understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

(h) Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs and Class Members.

167. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

168. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten years.

COUNT II
NEGLIGENCE *PER SE*
(Against All Defendants)

169. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

A. Negligence *Per Se* Under Section 5 of the FTC Act

170. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

171. Defendants violated §5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and disclosed and the foreseeable consequences of a data breach.

172. Plaintiffs and Class Members are consumers within the class of persons §5 of the FTC Act was intended to protect.

173. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

174. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

175. Defendants' violation of §5 of the FTC Act constitutes negligence *per se*.

176. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten years.

COUNT III
NEGLIGENCE *PER SE*
(Against Key Defendants)

177. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

A. Negligence *Per Se* Under the GLBA and Regulations

178. The GLBA states "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. §6801(a).

179. Key violated the GLBA and the Safeguards Rule by failing to use reasonable measures to protect PII and not complying with the industry standards. Key's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

180. Plaintiffs and Class Members are consumers within the class of persons the GLBA and the Safeguards Rule was intended to protect.

181. Moreover, the harm that has occurred is the type of harm that the GLBA and the Safeguards Rule was intended to guard against.

182. As a direct and proximate result of Key's negligence, Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

183. Key's violation of GLBA and the Safeguards Rule constitutes negligence *per se*.

184. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten years.

COUNT IV
BREACH OF IMPLIED CONTRACT
(Against All Defendants)

185. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

186. When Defendants required Plaintiffs and Class Members to supply their PII, Defendants entered into implied contracts with Plaintiffs and Class Members to protect the security of such information.

187. Defendants collect and use Plaintiffs' and Class Member's PII for the purpose of applying for and servicing a mortgage and/or refinancing as well as verifying whether Plaintiffs and Class Members have property insurance.

188. Such implied contracts arose from the course of conduct between Plaintiffs, Class Members, and Defendants.

189. The implied contracts required Defendants to safeguard and protect Plaintiffs' and Class Members' PII from being compromised and/or stolen.

190. Defendants did not safeguard or protect Plaintiffs' and Class Members' PII from being accessed, compromised, and/or stolen. Defendants did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiffs' and Class Members' PII.

191. Because Defendants failed to safeguard and/or protect Plaintiffs' and Class Members' PII from being compromised or stolen, Defendants breached their contracts with Plaintiffs and Class Members.

192. Plaintiffs and Class Members fully performed their obligations under the implied contracts by supplying their PII to Defendants.

193. As a direct and proximate result of Defendants' breaches of implied contracts, Plaintiffs and Class Members sustained damages as alleged herein and will continue to suffer damages as the result of Defendants' Data Breach.

194. Plaintiffs and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

195. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, among other things: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten years.

COUNT V
DECLARATORY JUDGMENT
(Against All Defendants)

196. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

197. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

198. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate. Defendants publicly deny these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

199. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Defendants owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, §5 of the FTC Act, the GLBA, and its regulations;

(b) Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

(c) Defendants' ongoing breaches of their legal duty continue to cause Plaintiffs harm.

200. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendants to:

(a) engage third party auditors, consistent with industry standards, to test their systems for weakness and upgrade any such weakness found;

(b) audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;

(c) regularly test their systems for security vulnerabilities, consistent with industry standards; and

(d) implement an education and training program for appropriate employees regarding cybersecurity.

201. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event Defendants are the subject of another data breach. The risk of

another such breach is real, immediate, and substantial. If Defendants suffer another breach, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

202. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damages. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

203. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction preventing Defendants from suffering another data breach would benefit the public, thus eliminating the additional injuries that would result to Plaintiffs and consumers, whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and all others similarly situated, pray for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representative of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: September 20, 2022

Respectfully submitted

s/ Alfred G. Yates, Jr.

Alfred G. Yates, Jr. (PA17419)
Gerald L. Rutledge (PA62027)
LAW OFFICE OF ALFRED G. YATES, JR., P.C.
1575 McFarland Road, Suite 305
Pittsburgh, PA 15216
Telephone: (412) 391-5164
Facsimile: (412) 471-1033
yateslaw@aol.com

Joseph P. Guglielmo (*pro hac vice* forthcoming)
Carey Alexander (*pro hac vice* forthcoming)
Ethan Binder (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212)223-6444
Facsimile: (212)-233-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com
ebinder@scott-scott.com

Counsel for Plaintiffs and the Proposed Class